

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**



DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁶ : H04L 9/06, 9/30		(11) Numéro de publication internationale: WO 99/48239
A1		(43) Date de publication internationale: 23 septembre 1999 (23.09.99)
(21) Numéro de la demande internationale: PCT/FR99/00613 (22) Date de dépôt international: 17 mars 1999 (17.03.99) (30) Données relatives à la priorité: 98/03242 17 mars 1998 (17.03.98) FR (71) Déposant (pour tous les Etats désignés sauf US): SCHLUMBERGER SYSTEMES [FR/FR]; 50, avenue Jean Jaurès, F-92120 Montrouge (FR). (72) Inventeur; et (75) Inventeur/Déposant (US seulement): SALLE, Patrick [FR/FR]; 46, rue d'Amblainvilliers, F-91370 Verrières-le-Buisson (FR). (74) Mandataire: MACQUET, Christophe; Schlumberger Systèmes, Test & Transactions, Boîte postale 620-04, F-92542 Montrouge Cedex (FR).		(81) Etats désignés: AU, CA, CN, JP, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Publiée Avec rapport de recherche internationale.

(54) Title: METHOD FOR DATA SECUREMENT USING A CRYPTOGRAPHIC ALGORITHM

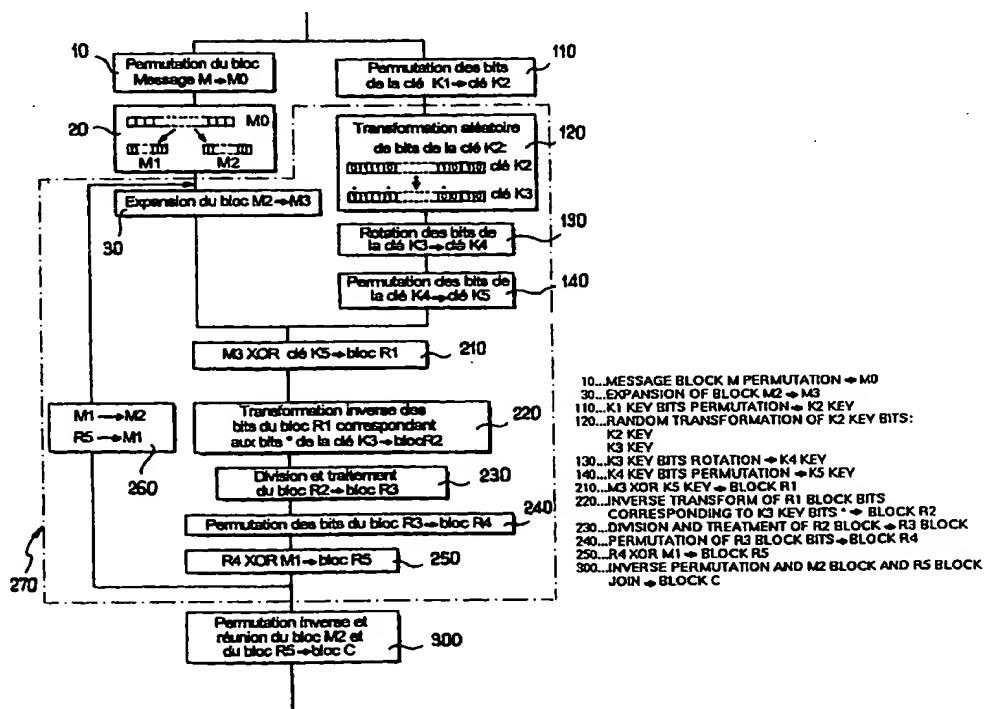
(54) Titre: PROCEDE DE SECURISATION DE DONNEES METTANT EN OEUVRE UN ALGORITHME CRYPTOGRAPHIQUE

(57) Abstract

The invention concerns a method for data securement using a cryptographic algorithm comprising at least a cycle executing repetitive operations of processing data elements (K2, R1) to produce encrypted information (C), said method comprising at least a step (120, 220) randomly modifying the execution of at least one operation from one cycle to the next or at least one of the data elements such that the encrypted information is unaltered by said random modification.

(57) Abrégé

L'invention concerne un procédé de sécurisation de données mettant en oeuvre un algorithme cryptographique comprenant au moins un cycle d'exécution d'opérations répétitives de traitement d'éléments de données (K2, R1) pour élaborer une information chiffrée (C), ce procédé comprenant au moins une étape (120, 220) de modification aléatoire de l'exécution d'au moins une opération d'un cycle à un autre ou d'au moins un des éléments de données de telle sorte que l'information chiffrée soit inchangée par cette modification aléatoire.



UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

PROCEDE DE SECURISATION DE DONNEES METTANT EN OEUVRE UN ALGORITHME CRYPTOGRAPHIQUE

5 La présente invention concerne un procédé de sécurisation de données, destiné par exemple à être mis en oeuvre par le microprocesseur d'une carte bancaire ou une carte d'autorisation d'accès lors d'une connexion à un terminal informatique d'authentification.

10 Les procédés de sécurisation de données de type connu mettent en oeuvre un algorithme cryptographique comprenant des cycles d'exécution d'opérations répétitives de traitement d'éléments de données contenus dans une mémoire de la carte pour élaborer une information chiffrée destinée à être communiquée au terminal informatique.

15 L'exécution du procédé par le microprocesseur de la carte engendre l'émission de signaux dérivés tels que des pics de consommation au niveau de l'alimentation électrique du microprocesseur, ou des variations du rayonnement électromagnétique de sorte que l'enveloppe du rayonnement électromagnétique est significative des données traitées. Un fraudeur désirant utiliser de façon non autorisée les cartes à microprocesseur peut lancer à plusieurs reprises l'exécution du procédé et
20 analyser les signaux dérivés émis pour établir des correspondances entre les différentes opérations de traitement et chaque signal ou série de signaux. A partir de ces correspondances, et en soumettant par exemple la carte à des perturbations électromagnétiques ou des baisses de tension à des instants précis du déroulement de l'algorithme, le fraudeur peut étudier l'information chiffrée obtenue et les différences,
25 ou au contraire l'absence de différences, entre les signaux dérivés émis pour découvrir les données contenues dans la mémoire de la carte.

 Pour compliquer une telle analyse des signaux dérivés, on a pensé à engendrer des signaux parasites venant s'ajouter aux signaux dérivés émis lors de l'exécution du procédé. L'extraction des signaux correspondant à l'exécution du procédé
30 est alors plus délicate mais demeure possible. On a également pensé à concevoir les composants électroniques de la carte et le programme d'exécution du procédé de sorte que les signaux dérivés émis soient indépendants de la valeur des données sensibles.

Toutefois, ceci complique la réalisation des cartes sans assurer une protection satisfaisante des données.

Un but de l'invention est de proposer un procédé de sécurisation efficace ne présentant pas les inconvénients précités.

5 En vue de la réalisation de ce but, on prévoit, selon l'invention, un procédé de sécurisation de données mettant en oeuvre un algorithme cryptographique d'exécution d'opérations de traitement d'éléments de données pour élaborer une information chiffrée, ce procédé comprenant au moins une étape de transformation aléatoire de l'exécution d'au moins une opération d'un cycle à un autre ou de
10 transformation aléatoire d'au moins un des éléments de données de telle sorte que l'information chiffrée soit inchangée par cette transformation aléatoire.

Par transformation aléatoire de l'exécution d'au moins une opération, on entend une modification de l'ordre d'exécution d'opérations ou de parties d'opérations, ou une modification du déroulement d'une seule opération. Ainsi, au moins une
15 opération et/ou au moins une des données traitées sont modifiées aléatoirement, ce qui affecte de façon aléatoire les signaux dérivés émis. Il est de ce fait très difficile pour un fraudeur de distinguer les différentes opérations de traitement et de découvrir les données à partir des signaux dérivés. En outre, la modification aléatoire n'affecte pas l'information chiffrée de sorte que celle-ci peut être utilisée de façon habituelle après
20 son élaboration.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description qui suit d'un mode de mise en oeuvre particulier non limitatif de l'invention, en relation avec la figure unique annexée illustrant sous forme d'un schéma par blocs le déroulement du procédé selon ce mode de mise en oeuvre.

25 Le procédé de sécurisation selon l'invention est ici décrit mettant en oeuvre un algorithme cryptographique symétrique de type DES (abréviation des termes DATA ENCRYPTION STANDARD) en vue d'élaborer une information chiffrée C de 64 bits à partir d'un bloc message M et d'une clé secrète K1 eux-mêmes de 64 bits.

Le procédé débute par la permutation 10 des bits du bloc message M
30 entre eux pour former le bloc M0.

Le bloc M0 est alors divisé en deux blocs M1 et M2 de 32 bits lors d'une étape de division 20.

Il est ensuite procédé à l'expansion 30 du bloc M2 pour former un bloc M3 de 48 bits. Cette expansion 30 est par exemple réalisée en découpant le bloc M2 en huit quartets et en ajoutant à chaque quartet le bit extrême adjacent des quartets encadrant le quartet concerné (les quartets extrêmes étant considérés comme adjacentes).

Parallèlement à ces opérations, une permutation 110 est effectuée sur les bits de la clé K1 pour former la clé K2. Les bits non significatifs de la clé K1 sont simultanément supprimés de sorte que la clé K2 a seulement 56 bits.

Selon l'invention, les bits de la clé K2 sont alors modifiés aléatoirement lors d'une transformation 120. Les bits de la clé K3 correspondant aux bits modifiés de la clé K2, ici marqués par une étoile, sont mémorisés. La transformation aléatoire 120 est par exemple réalisée en associant à la clé K2, par l'intermédiaire d'un opérateur logique de type OU exclusif, un nombre aléatoire engendré par un générateur de nombres non prédictibles de la carte.

Une clé K4 est obtenue par la rotation 130 des bits de la clé K3. Puis, une permutation 140 est réalisée sur les bits de la clé K4 pour former la clé K5. Simultanément à la permutation 140, les bits non significatifs de la clé K4 sont éliminés de sorte que la clé K5 comporte 48 bits.

Le procédé se poursuit par l'association 210 du bloc M3 et de la clé K5 par l'intermédiaire d'un opérateur logique de type OU exclusif. Le résultat de cette association est le bloc R1.

La transformation inverse des bits du bloc R1 correspondant aux bits modifiés par la transformation 120 est ensuite réalisée pour former le bloc R2. Cette transformation 220 inverse de la transformation 120 vise à remettre les bits du bloc R1 correspondant aux bits marqués d'une étoile dans l'état dans lequel ils auraient été en l'absence de la transformation 120.

Il est ensuite procédé, de façon classique, à la division et au traitement 230 du bloc R2, à la permutation 240 des bits du bloc R3 formés lors de l'étape 230, et à l'association 250 du bloc R4 résultat de l'étape 240 au bloc M1 par un opérateur OU exclusif pour former le bloc R5.

Le groupe d'opérations, désigné de manière générale par la référence 270, est ensuite exécuté à nouveau à quinze reprises en affectant, à chacune de celles-ci,

la valeur du bloc M1 au bloc M2 et la valeur du bloc R5 au bloc M1 lors d'une étape d'affectation 260.

Le procédé se termine par l'opération 300 d'obtention de l'information chiffrée C par la permutation inverse et la réunion du bloc dernier M2 et du bloc
5 dernier R5 obtenus.

On comprend que l'étape de modification aléatoire de la clé K2 comprend la phase de transformation 120 et la phase de transformation inverse 220. Ces deux phases permettent d'obtenir une information chiffrée C qui n'est pas affectée par cette modification aléatoire.

10 On pourrait également réaliser de la même manière une modification aléatoire du bloc M2 et/ou d'une autre donnée.

Selon un autre mode de mise en oeuvre de l'invention, lequel peut être associé à une étape de modification telle que précédemment décrite, l'exécution d'au moins une opération peut être modifiée de façon aléatoire d'un cycle à l'autre, un cycle
15 pouvant être un cycle complet d'exécution de l'algorithme ou un cycle intermédiaire d'exécution d'un groupe d'opérations.

Par exemple, une détermination aléatoire de l'ordre d'exécution de certaines opérations peut être réalisée au cours d'un cycle d'exécution de l'algorithme. Les opérations retenues seront celles dont l'ordre d'exécution les unes par rapport aux
20 autres n'influent pas sur le résultat. Pour réaliser cette détermination, on pourra prévoir à la fin des opérations choisies un saut conditionnel vers certaines opérations en fonction de la valeur d'un nombre aléatoire ou définir un tableau des adresses des différentes opérations parcouru de façon aléatoire.

A titre d'exemple, la permutation 10 des bits du bloc message M
25 pourrait être effectuée après la permutation 110 des bits de la clé K1 ou inversement.

De même, il pourrait être prévu une détermination aléatoire de l'ordre d'exécution des opérations du groupe 270 pour chaque cycle intermédiaire d'exécution de celles-ci (16 cycles intermédiaires d'exécution de ces opérations pour un cycle complet d'exécution de l'algorithme). Là encore, l'ordre d'exécution de ces opérations
30 sera choisi pour ne pas influencer sur le résultat.

Par ailleurs, pour certaines opérations, les données sont traitées par éléments. Ainsi, lors de l'expansion 30, les blocs M2 sont traités par quartets. Lors de

cette opération, on peut prévoir de déterminer aléatoirement l'ordre de traitement des différents quartets. De même, lors de la permutation 140 les bits de la clé K4 sont traités individuellement. Une étape de détermination aléatoire de l'ordre de traitement des bits peut également être prévue pour l'exécution de cette permutation. Les quartets
5 du bloc M2 peuvent également être traités en alternance avec les bits de la clé K4, c'est-à-dire que l'on traite par exemple un premier quartet du bloc M2 puis une série de bits de la clé K4, puis un deuxième quartet du bloc M2 etc., en mémorisant à chaque fois les éléments de donnée traités afin de contrôler que toutes les opérations requises sont bien exécutées.

10 Bien entendu, l'invention n'est pas limitée au mode de réalisation qui vient d'être décrit, mais englobe au contraire toute variante reprenant, avec des moyens équivalents, ses caractéristiques essentielles.

En particulier, bien que l'invention ait été décrite en relation avec un algorithme de type DES, l'invention peut être appliquée à d'autres algorithmes
15 symétriques qui procèdent par modification de bits. Ainsi, la modification étant effectuée au moyen d'un opérateur logique du type OU EXCLUSIF, la longueur des éléments de données non transformés est identique à la longueur de ces éléments de données transformés.

De plus, les nombres de bits des données ne sont mentionnés qu'à titre
20 indicatif et peuvent être modifiés pour être adaptés au degré de sécurisation envisagé.

On notera par ailleurs que tous les éléments de données M, M0, M1, M2, M3, K1, K2, K3, K4, K5, R1, R2, R3, R4 et R5 peuvent être transformés en leur associant, par l'intermédiaire de l'opérateur logique OU EXCLUSIF, un nombre aléatoire sachant que, postérieurement à cette étape de transformation aléatoire, on
25 procédera à une étape de transformation inverse de sorte que l'information chiffrée C soit inchangée par lesdites transformations.

En particulier, les éléments de données peuvent être des clés K1, K2, K3, K4, K5 ou des blocs de message M, M0, M1, M2, M3 ou des blocs de messages associés à une clé par un opérateur logique du type OU EXCLUSIF R1, R2, R3, R4,
30 R5.

On notera enfin que, si l'étape de transformation aléatoire est une étape préalable au groupe d'opérations exécuté à plusieurs reprises et si l'étape de

transformation inverse est une étape postérieure audit groupe d'opérations, il suffit de générer un nombre aléatoire une fois et de traiter le bloc de message M par l'algorithme pour obtenir une information chiffrée, tous les éléments de données du bloc étant modifiés. La chaîne des données est protégée de bout en bout. En outre, en ne
5 multipliant pas les étapes de transformation et le nombre de nombres aléatoires générés, l'algorithme est mis en oeuvre rapidement, ce qui est nécessaire dans le cas d'une carte à puce où la durée de l'exécution d'un algorithme doit être minimale.

REVENDEICATIONS

1. Procédé de sécurisation de données (M) mettant en oeuvre, dans un microprocesseur d'une carte à puce, un algorithme cryptographique d'exécution d'opérations de traitement d'éléments de données (M, M0, M1, M2, M3, K1, K2, K3, K4, K5, R1, R2, R3, R4, R5) pour élaborer une information chiffrée (C), caractérisé en ce qu'il comprend au moins, d'une part, une étape de transformation (120) aléatoire de bits d'au moins un des éléments de données (K2) en associant audit élément de données (K2), par l'intermédiaire d'un opérateur logique du type OU EXCLUSIF, un nombre aléatoire, et, d'autre part, postérieurement à cette étape de transformation aléatoire, une
10 étape de transformation inverse (220), de telle sorte que l'information chiffrée (C) soit inchangée par ces étapes de transformation (120, 220).

2. Procédé de sécurisation selon la revendication 1, caractérisé en ce qu'un élément de données transformé de manière aléatoire est une clé (K1, K2, K3, K4, K5).

3. Procédé de sécurisation selon l'une des revendications 1 ou 2, caractérisé en ce qu'un élément de données transformé de manière aléatoire est un bloc de message (M, M0, M1, M2, M3).
15

4. Procédé de sécurisation selon l'une des revendications 1, 2 ou 3, caractérisé en ce qu'un élément de données transformé de manière aléatoire est un bloc de message associé à une clé par un opérateur logique du type OU EXCLUSIF (R1, R2, R3, R4, R5).
20

5. Procédé de sécurisation selon l'une des revendications précédentes, caractérisé en ce que l'algorithme cryptographique d'exécution d'opérations de traitement de données (M, M0, M1, M2, M3, K1, K2, K3, K4, K5, R1, R2, R3, R4, R5) comprend un groupe d'opérations (270) exécuté à plusieurs reprises.

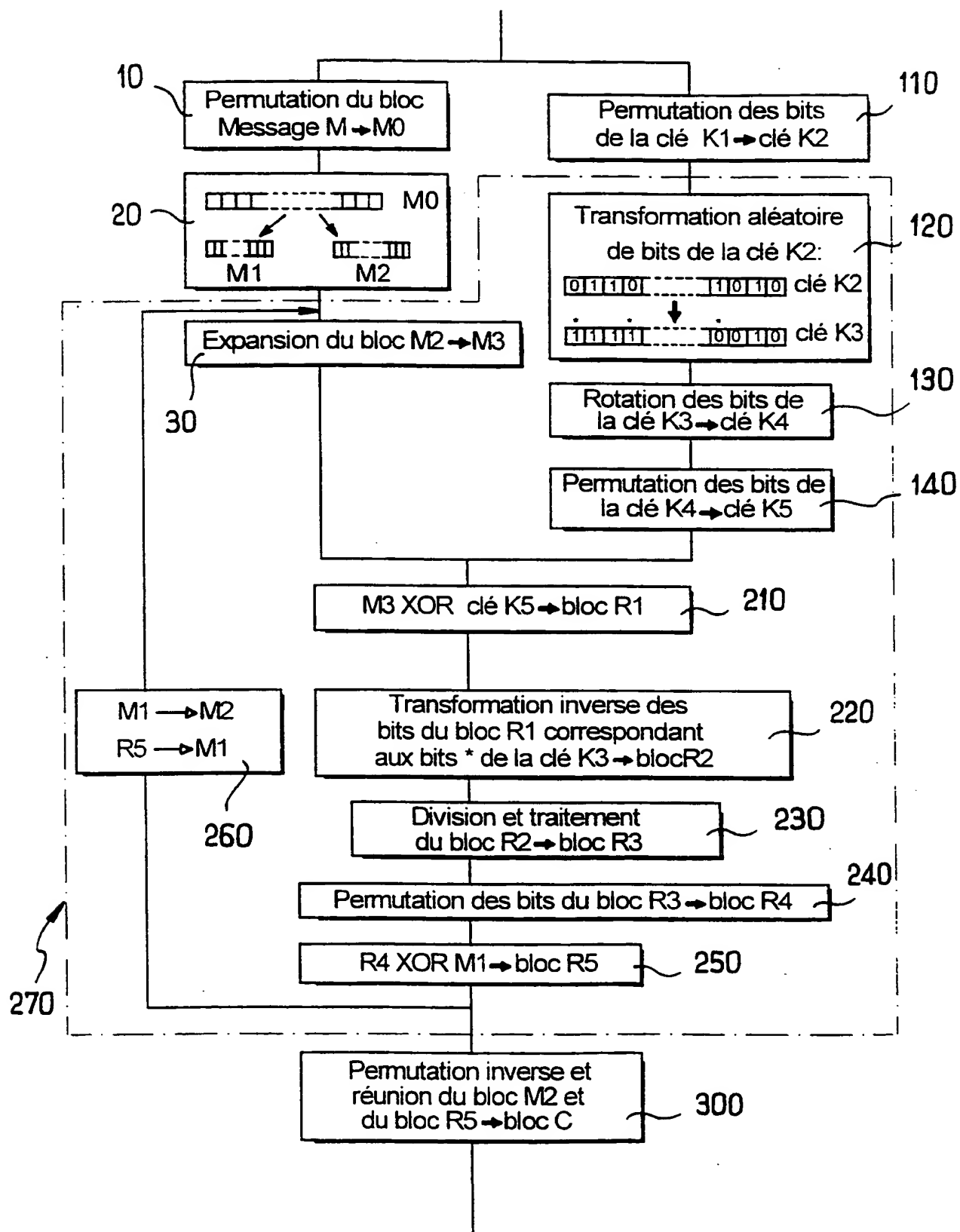
6. Procédé de sécurisation selon la revendication 5, caractérisé en ce que l'étape de transformation aléatoire est une étape préalable au groupe d'opérations (270) exécuté à plusieurs reprises et en ce que l'étape de transformation inverse est une étape postérieure audit groupe d'opérations (270).
25

7. Procédé de sécurisation selon l'une des revendications précédentes, caractérisé en ce qu'il comprend en outre une étape de modification aléatoire de l'ordre d'exécution des opérations du groupe d'opérations (270).
30

8. Procédé de sécurisation selon l'une des revendications précédentes, caractérisé

en ce que l'algorithme cryptographique est du type DATA ENCRYPTION STANDARD.

1 / 1



INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 99/00613

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/06 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KOCHER P C: "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems" ADVANCES IN CRYPTOLOGY - CRYPTO'96. 16TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, SANTA BARBARA, CA, USA, 18-22 AUG. 1996, pages 104-113, XP000626590 ISBN 3-540-61512-1, 1996, Berlin, Germany, Springer-Verlag, Germany see abstract see page 111, line 23 - last line see page 112, paragraph 3	1,5

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

15 June 1999

Date of mailing of the international search report

21/06/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Holper, G

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No

PCT/FR 99/00613

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 H04L9/06 H04L9/30

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 6 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	KOCHER P C: "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems" ADVANCES IN CRYPTOLOGY - CRYPTO'96. 16TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, SANTA BARBARA, CA, USA, 18-22 AUG. 1996, pages 104-113, XP000626590 ISBN 3-540-61512-1, 1996, Berlin, Germany, Springer-Verlag, Germany voir abrégé voir page 111, ligne 23 - dernière ligne voir page 112, alinéa 3 -----	1,5

☐ Voir la suite du cadre C pour la fin de la liste des documents

☐ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

15 juin 1999

Date d'expédition du présent rapport de recherche internationale

21/06/1999

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Holper, G